IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product embodied on a tangible computer readable medium for controlling operation of a computer to detect malware, said computer program product comprising:

pending scan database code operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed;

scanning code operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database as having been written to the data storage device and for which the scan for malware has yet to be performed; and

file read code operable in response to a read request for a computer file identified within said pending scan database to trigger said scanning code to scan said computer file as a high priority task with a first priority that is higher than a second priority of said low priority task, before permitting read access to said computer file;

wherein an order of said computer files identified within said pending scan database being scanned is based on an algorithm that estimates the likelihood of said read request being performed on each computer file.

2. (Previously Presented) A computer program product as claimed in claim 1, further comprising file write code operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.

3. (Cancelled)

4. (Original) A computer program product as claimed in claim 1, further comprising scanned file database code operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.

5. (Original) A computer program product as claimed in claim 4, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

6. (Previously Presented) A computer program product as claimed in claim 5, wherein said file read code is further operable in response to said read request for said computer file to detect if said computer file is within said scanned file database, to recalculate a checksum value for said computer file, and to determine that said recalculated checksum value matches a stored checksum within said scanned file database before permitting said read request.

7. (Original) A computer program product as claimed in claim 4, further comprising initiation code operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

8. (Previously Presented) A computer program product as claimed in claim 1, wherein said malware comprises one or more of:

a computer file infected with a computer virus;

a Trojan;

a banned computer file; and

a computer file containing banned content.

9. (Currently Amended) A method for detecting malware, said method comprising the steps of:

maintaining a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed;

as a low priority task within a multitasking environment, conducting malware scanning upon computer files identified within said pending scan database as having been written to the data storage device and for which the scan for malware has yet to be performed; and

in response to a read request for a computer file identified within said pending scan database, triggering scanning of said computer file as a high priority task with a first priority that is higher than a second priority of said low priority task, before permitting read access to said computer file;

wherein an order of said computer files identified within said pending scan database being scanned is based on an algorithm that estimates the likelihood of said read request being performed on each computer file.

10. (Original) A method as claimed in claim 9, further comprising the step of as a computer file is written to a storage device adding data identifying said computer file to said pending scan database.

11. (Cancelled)

12. (Original) A method as claimed in claim 9, further comprising maintaining a scanned file database storing data identifying computer files that have been scanned for malware.

13. (Original) A method as claimed in claim 12, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

14. (Previously Presented) A method as claimed in claim 13, further comprising the step of in response to said read request for said computer file, detecting if said computer

file is within said scanned file database, recalculating a checksum value for said computer file, and determining that said recalculated checksum value matches a stored checksum within said scanned file database before permitting said read request.

15. (Original) A method as claimed in claim 12, further comprising the step of upon startup detecting any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

16. (Previously Presented) A method as claimed in claim 9, wherein said malware comprises one or more of:

a computer file infected with a computer virus;

a Trojan;

a banned computer file; and

a computer file containing banned content.

17. (Currently Amended) Apparatus for detecting malware, said apparatus comprising:

pending scan database logic operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed;

scanning logic operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database as having been written to the data storage device and for which the scan for malware has yet to be performed; and

file read logic operable in response to a read request for a computer file identified within said pending scan database to trigger said scanning logic to scan said computer file as a high priority task with a first priority that is higher than a second priority of said low priority task, before permitting read access to said computer file;

wherein an order of said computer files identified within said pending scan database being scanned is based on an algorithm that estimates the likelihood of said read request being performed on each computer file.

18. (Original) Apparatus as claimed in claim 17, further comprising file write logic operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.

19. (Cancelled)

20. (Original) Apparatus as claimed in claim 17, further comprising scanned file database logic operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.

21. (Original) Apparatus as claimed in claim 20, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

22. (Previously Presented) Apparatus as claimed in claim 21, wherein said file read logic is further operable in response to said read request for said computer file to detect if said computer file is within said scanned file database, to recalculate a checksum value for said computer file, and to determine that said recalculated checksum value matches a stored checksum within said scanned file database before permitting said read request.

23. (Original) Apparatus as claimed in claim 20, further comprising initiation logic operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

24. (Previously Presented) Apparatus as claimed in claim 17, wherein said malware comprises one or more of:

a computer file infected with a computer virus;

a Trojan;

a banned computer file; and

a computer file containing banned content.

25. (Cancelled)

26. (Previously Presented) A computer program product as claimed in claim 4, wherein only computer files determined to be clean from the malware scanning are stored in the scanned file database.

27. (Cancelled)

28. (Previously Presented) A computer program product as claimed in claim 1, wherein if said scanning code determines that said computer file is clean, said data identifying said computer file is removed from said pending scan database.

29. (Previously Presented) A computer program product as claimed in claim 1, wherein actions are triggered if said scanning code determines that said computer file is not clean.

30. (Previously Presented) A computer program product as claimed in claim 29, wherein said malware actions include at least one of file cleaning, file quarantining, file deletion, and alert message issuing.

31. (Previously Presented) A computer program product as claimed in claim 1, wherein said second priority of said low priority task is determined based on a predetermined time period.